Troubleshooting de Falha de Mídia para Chamadas Através de Expressways quando a Inspeção SIP está ativada

Contents

Introduction

Este documento descreve como desabilitar a inspeção do Session Initiation Protocol (SIP) em firewalls Adaptive Security Appliance (ASA).

Informações de Apoio

A finalidade da inspeção SIP é fornecer tradução de endereços no cabeçalho e no corpo do SIP para permitir a abertura dinâmica de portas no momento da sinalização SIP. A inspeção SIP é uma camada extra de proteção que não expõe IPs internos à rede externa quando você faz chamadas de dentro da rede para a Internet. Por exemplo, em uma chamada Business-to-Business de um dispositivo registrado para o Cisco Unified Communications Manager (CUCM) através do Expressway-C e para o Expressway-E discando um domínio diferente, esse endereço IP privado no cabeçalho SIP é convertido para o IP do seu firewall. Muitos sintomas podem surgir com o ASA que inspeciona a sinalização SIP, criando falhas de chamada e áudio ou vídeo unidirecionais.

Falha de Mídia para Chamadas sobre Expressways quando a Inspeção SIP está ativada

Para que a parte chamadora decifre para onde enviar a mídia, ela envia o que espera receber em um Session Description Protocol (SDP) no momento da negociação do SIP para áudio e vídeo. Em um cenário de oferta antecipada, ele envia mídia com base no que recebeu no 200 OK, como mostrado na imagem.

Quando a inspeção SIP é ativada por um ASA, o ASA insere seu endereço IP no parâmetro c do SDP (informações de conexão para retornar chamadas) ou no cabeçalho SIP. Aqui está um exemplo de como uma chamada com falha é quando a Inspeção SIP é ativada:

```
SIP INVITE:

|INVITE sip:7777777@domain SIP/2.0

Via: SIP/2.0/TCP *EP IP*:5060

Call-ID: faece8b2178da3bb

CSeq: 100 INVITE

Contact: <sip:User@domain;

From: "User" <sip:User@domain >;tag=074200d824ee88dd

To: <sip:7777777@domain>

Max-Forwards: 15

Allow: INVITE,ACK,CANCEL,BYE,INFO,OPTIONS,REFER,NOTIFY

User-Agent: TANDBERG/775 (MCX 4.8.12.18951) - Windows

Supported: replaces,timer,gruu

Session-Expires: 1800

Content-Type: application/sdp

Content-Length: 1961
```

Aqui o firewall insere seu próprio endereço IP público e substitui o domínio no cabeçalho da mensagem de confirmação (ACK):

```
SIP ACK:

|ACK sip:7777777@*Firewall IP 5062;transport=tcp SIP/2.0
```

```
Via: SIP/2.0/TLS +Far End IP*:7001

Call-ID: faece8b2178da3bb

CSeq: 100 ACK

From: "User" <sip:User@domain>;tag=074200d824ee88dd

To: <sip:7778400@domain>;tag=1837386~f30f6167-11a6-4211-aed0-632da1f33f58-61124999

Max-Forwards: 68

Allow: INVITE,ACK,CANCEL,BYE,INFO,OPTIONS,REFER,NOTIFY

User-Agent: TANDBERG/775 (MCX 4.8.12.18951) - Windows

Supported: replaces,100rel,timer,gruu

Content-Length: 0
```

Se o endereço IP público do firewall for inserido em qualquer lugar dentro desse processo de sinalização SIP, as chamadas falharão. Também pode não haver ACK enviado de volta do cliente do agente de usuário se a inspeção SIP estiver ativada, o que resulta em falha de chamada.

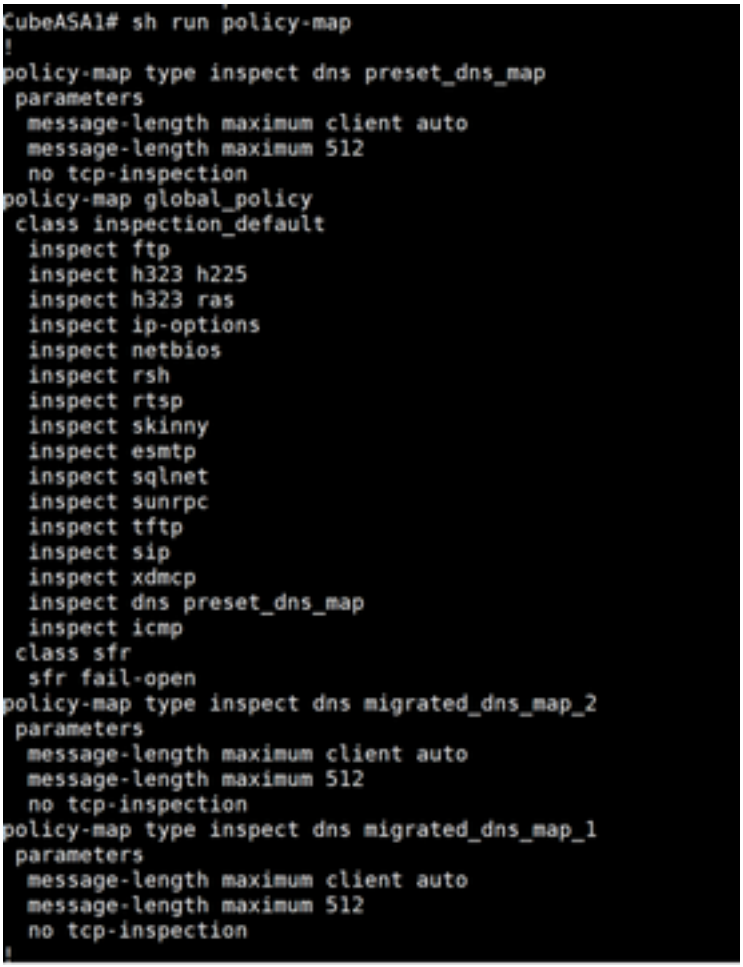
Solução

Para desabilitar a Inspeção SIP em um Firewall ASA:

Etapa 1. Faça login no CLI do ASA.

Etapa 2. Execute o comando **show run policy-map**.

Etapa 3. Verifique se inspect sip está na lista global-policy do mapa de políticas, como mostrado na imagem.



Etapa 4. Se estiver, execute estes comandos:

CubeASA1#policy-map global_policy

CubeASA1#class inspection_default

CubeASA1#no inspect sip

Informações Relacionadas

- Não é recomendável usar a inspeção SIP em um firewall ASA (Página 74); https://www.cisco.com/c/dam/en/us/td/docs/telepresence/infrastructure/vcs/config_guide/X8-11/Cisco-VCS-Basic-Configuration-Control-with-Expressway-Deployment-Guide-X8-11-4.pdf
- Mais informações sobre a inspeção do SIP podem ser encontradas aqui; https://www.cisco.com/c/en/us/td/docs/security/asa/asa99/configuration/firewall/asa-99-firewall-config/inspect-voicevideo.pdf
- **Suporte Técnico e Documentação - Cisco Systems**